



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/825,139	04/03/2001	David J. Wetherall	0016.0007.US1	1582
29127	7590	01/24/2008		
HOUSTON ELISEEVA 4 MILITIA DRIVE, SUITE 4 LEXINGTON, MA 02421			EXAMINER BARQADLE, YASIN M	
			ART UNIT 2153	PAPER NUMBER
			MAIL DATE 01/24/2008	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/825,139
Filing Date: April 03, 2001
Appellant(s): WETHERALL ET AL.

MAILED

JAN 24 2008

Technology Center 2100

J. Grant Houston
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 11/08/2007 appealing from the Office action
mailed February 6, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,598,077	Primak	07-2003
20020108059	Canion	082002
6,799,270	Bull	9-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 10-11, 17-19, 22, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Primak et al USPN (6598077) in view of Canion et al USPN. (20020108059).

As per claim 1, and 17, Primak teaches in a routing device (dynamic route 10), a method of operation comprising:

receiving a packet sent by a client device [a client's request for dynamic content to the dynamic content router. (The dynamic content router then determines the appropriate application server or application cluster for the client's request based on number of factors, including but not limited to the content availability, data server's capacity and session persistence. Col. 3, lines 59 to col. 4, line 5);

determining if the packet is destined for a server of interest by reference to a destination address of the packet (When a session is established between the client and the selected application server, the dynamic content router examines the session communications to

determine or extract a client identifier (also referred to herein as a content identifier). The dynamic content router utilizes the content identifier to determine if the client is already logged onto one of the application servers on the site col. 4, lines 16-26 and col. 6, lines 9-34); if the packet is not destined for the server of interest, routing the packet to its destination; if the packet is determined to be destined for the server of interest, routing the packet to its destination (col. 6, lines 35-43), independently determining whether said packet is a part of a conversation between the client device and the server of interest based at least in part on persistent information included in said packet [However, since the client request includes session ID, the dynamic router 10 can extract the session ID from the client request. The extracted session ID then can be used by the dynamic router 10 to search the session label 12 to find corresponding content label. That is, once the session ID is found in the session table 12, the dynamic content router can use the link to locate the content label associated with this client and thereafter determine the dynamic content based on the content label. (Col. 6, lines 9-34); and handling the packet based at least in part on the result of said independent determination by forwarding the packet to if the packet is deemed to be part of a conversation between the client and the server (col. 6, lines 9-42).

Although Primak shows substantial features of the claimed invention as explained above, he does not explicitly show dropping the packet if the packet is deemed to be undesirable packets.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Primak, as evidenced by Canion et al USPN. (20020108059).

In analogous art, Canion et al whose invention is about a system for detecting incoming data packets in a network, disclose a way of determining whether to forward or drop (discard) a packet through a network in response to a conversation identifier (received packet information) to protect the network against undesirable packets (packets with potential security violations) (§ 0174-0177 and ¶ 0183-0187). Giving the teaching of Canion et al, a person of ordinary skill in the art would have readily recognized the desirability and the advantage of modifying Primak et al by employing the intrusion detection system of Canion et al in order to identify packets with potential security violations for the advantage of protecting the network against network security attacks such as denial of service attacks, sync attacks, ping attacks and unauthorized attacks (§ 0171 and ¶ 0183-0187).

As per claim 2 and 18, Primak et al teach the invention, wherein said independent determination comprises independently verifying a conversation identifier included in said packet based at least in part on other information included (col. 4, lines 16-26 and col. 6, lines 9-34).

As per claim 3 and 19, Primak et al teach the invention, wherein said independent verification comprises independently regenerating the conversation identifier using at least said other information included in said packet; and

comparing the independently re-generated conversation identifier with the included conversation identifier [col. 9, lines 20-46).

As per claim 11 and 22, Primak et al teaches a method of operation comprising:

at least one processor (10, 20, 30, fig. 2);

generating an independently verifiable conversation identifier for a packet destined for a client device, using at least persistent information that will be included in said packet [col. 9, lines 20-46);

including the independently verifiable conversation identifier with said packet for use by the client device to include in a subsequent packet sent by the client device destined for the server [col. 4, lines 16-26 and col. 6, lines 9-34]; and

transmitting said independently verifiable conversation identifier included packet to said client device (col. 4, lines 16-26 and col. 6, lines 9-34);

Primak et al further teach a summation unit to insert the independently verifiable conversation identifier with a packet [col. 7, lines 63 to col. 8, lines 9 and col. 11, lines 41-56]; determining if the packet is destined for a server of interest by reference to a destination address of the packet (When a session is established between the client and the selected application server, the dynamic content router examines the session communications to determine or extract a client identifier (also referred to herein as a content identifier). The dynamic content router utilizes the content identifier to determine if the client is already logged onto one of the application servers on the site (col. 4, lines 16-26 and col. 6, lines 9-34); if the packet is not destined for the server of interest, routing the packet to its destination; if the packet is determined to be destined for the server of interest, routing the packet to its destination (col. 6, lines 35-43), independently determining whether said packet is a part of a conversation between the client device and the server of interest based at least in part on persistent information included in said

packet [However, since the client request includes session ID, the dynamic router 10 can extract the session ID from the client request. The extracted session ID then can be used by the dynamic router 10 to search the session table 12 to find corresponding content label. That is, once the session ID is found in the session table 12, the dynamic content router can use the link to locate the content label associated with this client and thereafter determine the dynamic content based on the content label (col. 6, lines 9-34).

Although Primak shows substantial features of the claimed invention as explained above, he does not explicitly show dropping the packet if the packet is deemed to be undesirable packets.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Primak, as evidenced by Canion et al USPN. (20020108059).

In analogous art, Canion et al whose invention is about a system for detecting incoming data packets in a network, disclose a way of determining whether to forward or drop a packet through a network in response to a conversation identifier (received packet information) to protect the network against undesirable packets (packets with potential security violations) (§ 0174-0177 and § 0183-0187). Giving the teaching of Canion et al, a person of ordinary skill in the art would have readily recognized the desirability and the advantage of modifying Primak et al by employing the intrusion detection system of Canion et al in order to identify packets with potential security violations for the advantage of protecting the network against network security attacks such as denial of service attacks, sync attacks, ping attacks and unauthorized attacks (§ 0171 and § 0183-0187).

As per claim 32, Canion et al as modified teach the invention, where the function unit (processing unit) drops packets that are not part of the conversation identifier to protect the server against receipt of undesirable packets (§ 0174-0177 and § 0183-0187).

Claims 4-9, 12-13 and 21, 23-25 rejected under 35 U.S.C. 103(a) as being unpatentable over Primak et al USPN (6598077) in view of Canion et al USPN. (20020108059) and further in view of Bull et al USPN (6799270).

As per claims 4 and 12, although Primak et al show substantial features of the claimed invention as explained in claim 1 and 11 above, they do not explicitly show a nonce.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the system disclosed by Primak et al, as evidenced by Bull et al USPN. (16799270).

In analogous art, Bull et al whose invention is about a system for securely distributing session keys over a network of a chain of nodes including client nodes (14), server nodes (18) and intermediate nodes (18), disclose a bit string of data that includes a nonce (randomly generated value that is concatenated to the end of a message) that is used for identification and verification purpose [Col. 6, lines 39-50 and col. 7, lines 21-60]. Giving the teaching of Bull et al, a person of ordinary skill in the art would have readily recognized the desirability and the advantage of modifying Primak et al by employing the system of Bull et in order to generate a unique value

that identifies a client session and to verify the integrity of the response coming from the server [Col. 6, lines 39-50 and col. 7, lines 29-35].

Bull et al further teaches said re-generating the nonce using a deterministic function with a sequence number of the nonce and a plurality of persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function [Col. 5, lines 9-34 and Col. 6, lines 7-65].

As per claims 5, 13 and 24, Primak et al teach the invention, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number [client session (packet) with web server inherently includes a source address, a destination address and a port number].

As per claim 6, Bull et al further teach the invention as explained in claim 4 above, wherein the method further comprises at least one of receiving into said routing device said secret value, and equipping/configuring said routing device with said deterministic function [Col. 5, lines 9-34 and Col. 6, lines 7-65].

As per claim 7 and 25, Bull et al further teaches the invention, wherein said independent generation is performed using a selected one of a message authentication code function and an universal hash function [col. 5, lines 39 to Col. 6, lines 7-47].

As per claim 8, Primak et al as modified teach the invention, wherein the method further comprises recording a time of first observation for the nonce if the nonce is a newly observed nonce [col. 9, lines 20-67].

As per claim 9, Primak et al as modified teach the invention, wherein the method further comprises determining if time has elapsed more than a predetermined threshold since a time of first observation was recorded for the nonce, if the extracted nonce and the independently generated nonce are deemed to be the same [col. 9, lines 20-67].

As per claims 20-21 and 23, these claims include similar limitations as claim 4 and 12 above. Therefore, they are rejected with the same rationale.

(10) Response to Argument

Appellant argues, “Neither of the applied references shows or suggests this claimed functionality of forwarding or dropping a packet to a particular server of interest in dependence upon whether the packet is part of an existing conversation between the client sending the packet and the server of interest by reference to persistent information included in the packet.” (Page 8, second paragraph). Appellant continues to argue that “The Canion Application also fails to show or suggest the feature of forwarding or dropping packets in dependence upon whether the packets are part of an existing conversation.” (Page 8, last paragraph).

Examiner notes that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Primak is relied upon to teach the claimed functionality of forwarding or dropping a packet to a particular server of interest in dependence upon whether the packet is part of an existing conversation between the client sending the packet and the server of interest by reference to persistent information included in the packet. For example, Primak teaches "When a session is established between the client and the selected application server, the dynamic content router examines the session communications to determine or extract a client identifier (also referred to herein as a content identifier)". (col. 6, lines 9-34). Primak further teaches "The dynamic content router 10a compares the session ID in the client's request against the entries in its session Table 12. If a matching session record is found the dynamic content router 10a instructs the plug-in 22b to route the request to the application server 30 corresponding to the session server ID of the matching session record namely the application server 30a in this case." (col. 11, lines 14-40). Primak further teaches "Each time a request for content is received from the client 60 the dynamic content router 10 examines the header of the request for a session ID. If the request contains a session ID, the dynamic content router 10 compares the session ID against the entries in the session table 12. If the session ID of the request matches a session ID in one of the session records stored in the session table 12, the dynamic content router 10 instructs the plug-in 22b to route the request to the application server associated with the session server ID in the matching session record." (Col. 8, lines 29-47). Therefore, Primak clearly teaches the claimed functionality of forwarding a packet to a particular server of interest (application server 30a) in dependence

upon whether the packet is part of an existing conversation between the client sending the packet (client 60) and the server of interest (application server 30a) by reference to persistent information included in the packet (based on the session information included in the client request. See fig. 2, fig. 5 and col. 11, lines 14-40).

As to the limitation of dropping packets, Canion is relied upon to teach this limitation. Canion teaches detecting incoming data packets in a network teaches a way of determining whether to forward or drop a packet through a network in response to a conversation identifier (received packet information) to protect the network against undesirable packets (packets with potential security violations) (§ 0177 and § 0187).

The Appellant also argues that "to be sure, the Canion Application does not suggest dropping packets. See Canion application at paragraph [0185]. The packets are dropped depending upon whether they are deemed to be part of an attack." This argument seems to be a contradicting statement. As indicated above Canion teaches detecting incoming data packets in a network and determining whether to forward if it is authentic or drop the packet if it is undesirable packet (packets with potential security violations to protect the network against) (§ 0177; § 0183 and § 0187). Therefore, the combined references of Primak and Canion teach the argued limitations.

The Appellant argues that "In short, Primak is not concerned with any verification at the client, but instead focuses on server system scaling." Examiner notes that Primak teaches "the present invention provides a system and method for identifying the dynamic content involved in every client request requiring access to the dynamic content." col. 2, lines 35-42. Primak examines each request (packet) to identify or determine the dynamic content that needs to be accessed."

col. 5, lines 50-66. This shows that Primak is interested in verifying the whole conversation between client 60 and the application servers.

Appellant also argues "Each of claims 1, 11, 17, and 22 requires determining if the packet is destined for a server of interest by reference to a destination address of the packet. In contrast, the Primak Patent teaches to route packets to a server in dependence upon a Session ID. See Primak Patent at col. 8, lines 45-48." (Page 9, second paragraph). Examiner agrees with the Appellant that "Primak Patent teaches to route packets to a server in dependence upon a Session ID, as indicated in Col. 8, lines 29-47 "the dynamic content router 10 routes the request to the application server associated with the session server ID in the matching session record."

This is typically the normal function of any routing device such as Primak's router 10 to check a packet's destination address field in order to forward the payload included in the packet to its destination address. The Appellant concedes this point at page 9 the last line of paragraph 3. "In contrast, the present invention is concerned with protecting a particular "server of interest" and thus routes packets based on the packet destination address field." In the summary of the claimed subject matter on page 2, paragraph 5 the Appellant refers to Drawings at Fig. 8, reference numeral 802, and Specification at page 12, line 5 to teach the above limitation. Fig. 8, reference numeral 802 simply recites "Destined for server of interest?" and Specification at page 12, line 5-7 recites " the intermediate routing device first determines if the packet is destined for a server of interest, block 802. That is, whether the destination addresses is addressed to a server..." The portions cited by the Appellant simply indicates the function of a routing device and as such Primak's dynamic router 10 is no different than the Appellant's routing device in terms of

routing a packet data based on packet destination address field. In fact, Primak in addition to performing the normal router function in forwarding packets based on their destination address, his dynamic content router routes packets to the particular application server associated with a session server ID in the matching session record (Col. 8, lines 29-47).

Regarding claim 4, Appellant argues "Moreover, there is no suggestion in the Primak and/or Bull Patents to forward or drop packets based on a conversation identifier generated based on a "preprovided secret value" and "values extracted from the packet" as claimed. (Page 10).

Examiner notes that the Appellant does not define secret value in the specification. Nonetheless, Bull in combination with Primak teaches "Each session key can be a randomly generated value used for signing messages or encryption. Only nodes possessing the same session key for decoding the encryption can understand encrypted communications. Consequently, two or more nodes having the same session key can communicate privately. Session keys exist only for the duration of a particular session (or conversation). ... In brief overview, in one embodiment the client node A 14 generates a request for authentication and for obtaining a session key and transmits the request to the first intermediate node B 22. The request includes both plain text and sealed text. The first intermediate node B 22 adds its authentication information to the original request from the client node A 14 to generate a new authentication request and forwards the new authentication request to the second intermediate node C 26" (Bull col. Col. 4, lines 65 to col. 5, line 21. See figs 7 and 8). Bull further teaches "Each node in the chain extracts and authenticates at least one session key directed to that node from the final response, and forwards the remainder of the response to the next node in the chain away from the server 18." See col. 5, lines 51-54.

Regarding claim 9, Appellant argues "However, the cited section of the Primak Patent does not seem to suggest that a packet should be dropped based on age of the conversation identifier in spite of the existence of a match for the conversation identifiers, as claimed. In short, the pending Office Action does not assert that the requirements of the claim are met by the reference and the reference does not show or suggest those requirements." (See age 11). Examiner notes that the combined teaching of Primak in view Canion and further in view of Bull teach the argued limitation. Fore example Primak teaches the aging factor [col. 9, lines 20-67] while Canion teaches the taking action such as discarding packets when undesirable packet are detected through "the MAC header identification and verification, IP header identification and verification, IP header checksum validation, TCP and UDP header identification and validation, and TCP or UDP checksum validation. It also may perform the lookup to determine the TCP connection or UDP socket (protocol session identifier) to which a received packet belongs. Thus, the network interface engine verifies packet lengths, checksums, and validity." (§ 065). Canion's system is flexible to take action such as discarding packets that are deemed undesirable in the network "It can take immediate action, such as discarding the packet or notifying the network administrator.... Thus, the security accelerator provides flexibility for providing counter measures to new security attacks as the new types of attacks become known." (§ 0177 and § 0183).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

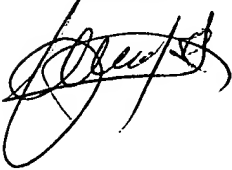
Application/Control Number:
09/825,139
Art Unit: 2153

Page 16


For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

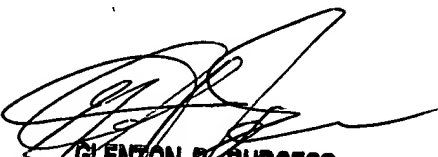
Y. Barqadle



Conferees:



LYNNE H. BROWNE
APPEAL PRACTICE SPECIALIST, TQAS
TECHNOLOGY CENTER 2100



GLENON B. BURGESS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100